



Windows 10

Índice

- 1. Nombre de la máquina**
- 2.Hash SHA-256**
- 3. Programa de control remoto**
 - 3.1 Fecha de descarga del fichero .exe**
 - 3.2 Fecha de ejecución del fichero.exe**
- 4. Fichero .ZIP eliminado**
- 5. Contraseñas débiles**
- 6. Conexión RDP**
 - 6.1 Puerto conexión máquina**
- 7. Conexión programa control remoto**
- 8.Fichero malicioso**

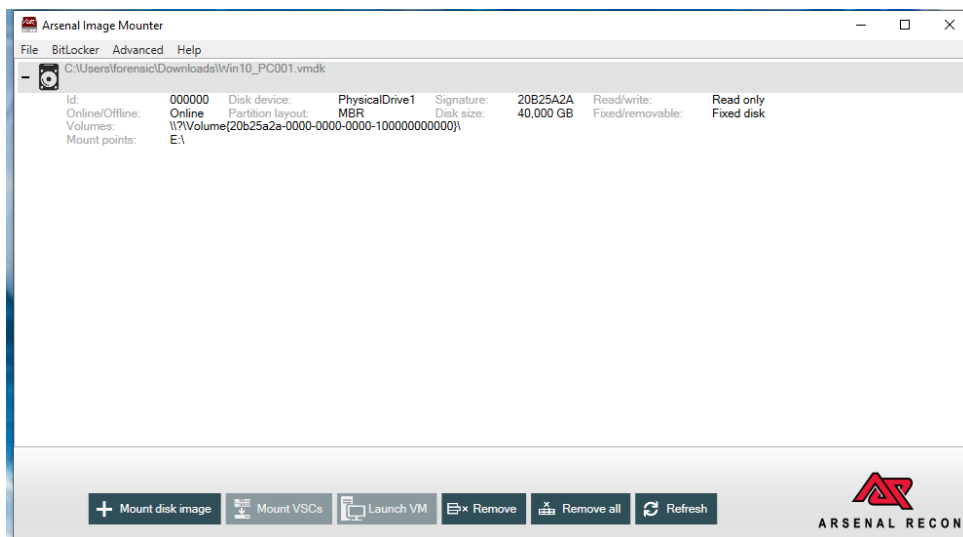
1. Nombre de la maquina:

Pegasus01 (kape)

El nombre de la máquina lo hemos conseguido a través del registro de logs que hemos sacado con Kape.

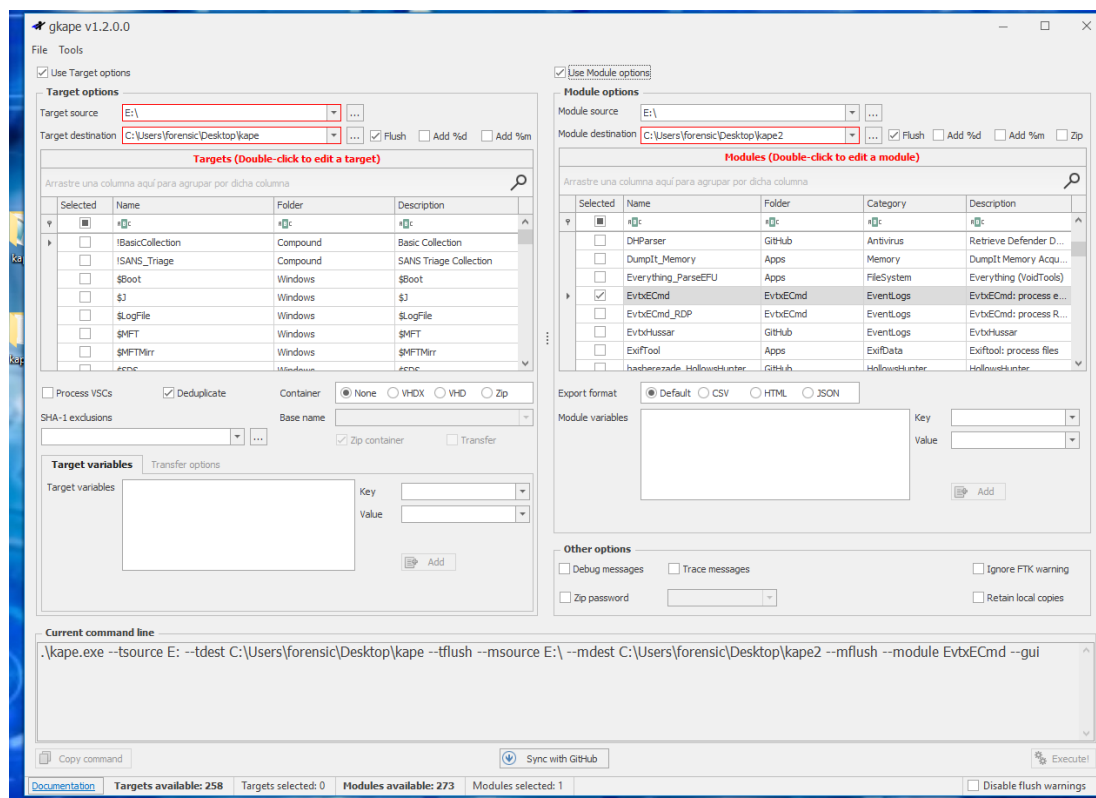
Pasos:

1º



Lo primero que hemos hecho es montar la imagen de la evidencia con la Herramienta Arsenal.

2º



Lo siguiente que hemos utilizado es la herramienta kape primero hemos ejecutado los targets y después las opciones de módulos, que hemos ejecutado la de EvtxECmd.

Al ejecutarlo nos ha extraído un fichero con varios logs y donde hemos conseguido descubrir el nombre de la máquina.

```
Archivo Máquina Ver Entradas Diagnostics Ayuda
20231230202234_EvtxECmd_Output.csv: Bloc de notas
Archivo Edición Formato Ver Ayuda
264,264,2022-04-29 16:43:46.5488622,1002,Warning,Microsoft-Windows-KnownFolders,Microsoft-Windows-Known Folders API Service,2480,2484,PEGASUS01,2,
265,265,2022-04-29 16:43:46.5493741,1002,Warning,Microsoft-Windows-KnownFolders,Microsoft-Windows-Known Folders API Service,2480,2484,PEGASUS01,2,
266,266,2022-04-29 16:43:46.5499778,1002,Warning,Microsoft-Windows-KnownFolders,Microsoft-Windows-Known Folders API Service,2480,2484,PEGASUS01,2,
267,267,2022-04-29 16:43:46.5506235,1002,Warning,Microsoft-Windows-KnownFolders,Microsoft-Windows-Known Folders API Service,2480,2484,PEGASUS01,2,
268,268,2022-04-29 16:43:46.5514774,1002,Warning,Microsoft-Windows-KnownFolders,Microsoft-Windows-Known Folders API Service,2480,2484,PEGASUS01,2,
269,269,2022-04-29 16:43:46.5529240,1002,Warning,Microsoft-Windows-KnownFolders,Microsoft-Windows-Known Folders API Service,2480,2484,PEGASUS01,2,
270,270,2022-04-29 16:43:46.5538020,1002,Warning,Microsoft-Windows-KnownFolders,Microsoft-Windows-Known Folders API Service,2480,2484,PEGASUS01,2,
271,271,2022-04-29 16:43:46.5545192,1002,Warning,Microsoft-Windows-KnownFolders,Microsoft-Windows-Known Folders API Service,2480,2484,PEGASUS01,2,
272,272,2022-04-29 16:43:46.5568219,1002,Warning,Microsoft-Windows-KnownFolders,Microsoft-Windows-Known Folders API Service,2480,2484,PEGASUS01,2,
273,273,2022-04-29 16:43:46.5580471,1002,Warning,Microsoft-Windows-KnownFolders,Microsoft-Windows-Known Folders API Service,2480,2484,PEGASUS01,2,
274,274,2022-04-29 16:43:46.7110136,1002,Warning,Microsoft-Windows-KnownFolders,Microsoft-Windows-Known Folders API Service,2480,2484,PEGASUS01,2,
275,275,2022-04-29 16:43:46.7182327,1002,Warning,Microsoft-Windows-KnownFolders,Microsoft-Windows-Known Folders API Service,2480,2484,PEGASUS01,2,
276,276,2022-04-29 16:43:46.7252006,1002,Warning,Microsoft-Windows-KnownFolders,Microsoft-Windows-Known Folders API Service,2480,2484,PEGASUS01,2,
277,277,2022-04-29 16:43:46.7260881,1002,Warning,Microsoft-Windows-KnownFolders,Microsoft-Windows-Known Folders API Service,2480,2484,PEGASUS01,2,
278,278,2022-04-29 16:43:46.7267888,1002,Warning,Microsoft-Windows-KnownFolders,Microsoft-Windows-Known Folders API Service,2480,2484,PEGASUS01,2,
279,279,2022-04-29 16:43:46.7280605,1002,Warning,Microsoft-Windows-KnownFolders,Microsoft-Windows-Known Folders API Service,2480,2484,PEGASUS01,2,
280,280,2022-04-29 16:43:54.3054947,1002,Warning,Microsoft-Windows-KnownFolders,Microsoft-Windows-Known Folders API Service,3588,3648,PEGASUS01,2,
281,281,2022-04-29 16:43:54.3098040,1002,Warning,Microsoft-Windows-KnownFolders,Microsoft-Windows-Known Folders API Service,3588,3648,PEGASUS01,2,
282,282,2022-04-29 16:43:54.3135525,1002,Warning,Microsoft-Windows-KnownFolders,Microsoft-Windows-Known Folders API Service,3588,3648,PEGASUS01,2,
283,283,2022-04-29 16:43:54.3140753,1002,Warning,Microsoft-Windows-KnownFolders,Microsoft-Windows-Known Folders API Service,3588,3648,PEGASUS01,2,
284,284,2022-04-29 16:43:54.3146740,1002,Warning,Microsoft-Windows-KnownFolders,Microsoft-Windows-Known Folders API Service,3588,3648,PEGASUS01,2,
285,285,2022-04-29 16:43:54.3153430,1002,Warning,Microsoft-Windows-KnownFolders,Microsoft-Windows-Known Folders API Service,3588,3648,PEGASUS01,2,
286,286,2022-04-29 16:43:54.3159629,1002,Warning,Microsoft-Windows-KnownFolders,Microsoft-Windows-Known Folders API Service,3588,3648,PEGASUS01,2,
287,287,2022-04-29 16:43:54.3172748,1002,Warning,Microsoft-Windows-KnownFolders,Microsoft-Windows-Known Folders API Service,3588,3648,PEGASUS01,2,
288,288,2022-04-29 16:43:54.3180353,1002,Warning,Microsoft-Windows-KnownFolders,Microsoft-Windows-Known Folders API Service,3588,3648,PEGASUS01,2,
289,289,2022-04-29 16:43:54.3185315,1002,Warning,Microsoft-Windows-KnownFolders,Microsoft-Windows-Known Folders API Service,3588,3648,PEGASUS01,2,
290,290,2022-04-29 16:43:54.3207915,1002,Warning,Microsoft-Windows-KnownFolders,Microsoft-Windows-Known Folders API Service,3588,3648,PEGASUS01,2,
291,291,2022-04-29 16:43:54.3217698,1002,Warning,Microsoft-Windows-KnownFolders,Microsoft-Windows-Known Folders API Service,3588,3648,PEGASUS01,2,
292,292,2022-04-29 16:43:54.3252291,1002,Warning,Microsoft-Windows-KnownFolders,Microsoft-Windows-Known Folders API Service,3588,3648,PEGASUS01,2,
293,293,2022-04-29 16:43:54.3298696,1002,Warning,Microsoft-Windows-KnownFolders,Microsoft-Windows-Known Folders API Service,3588,3648,PEGASUS01,2,
```

2. Hash SHA-256

4446e9c42345a32fa78a8ce20834faa047a3b161eba986f894d2230fcf6b0cbe

HashMyFiles							
File Edit View Options Help							
Filename	MD5	SHA1	CRC32	SHA-256	SHA-512	SHA-384	
Win10_PC001.vmdk	5ee316b95ad83f67ff1b511c372e2d5	c407c534116af248c730d3c246f81a6e2d31da...	573f0eeb	4446e9c42345a32fa78a8ce20834faa047a3b1...	8c091651de941af8cb2c37168730f3265ed64e...	3e8b29658d7646bd73dd8f234b7d0fe7a57c0...	Fi

Properties

Filename:

Win10_PC001.vmdk

MD5:

5ee316b95ad83f67ff1b511c372e2d5

SHA1:

c407c534116af248c730d3c246f81a6e2d31da1c

CRC32:

573f0eeb

SHA-256:

4446e9c42345a32fa78a8ce20834faa047a3b161eba986f894d2230fcf6b0cbe

SHA-512:

8c091651de941af8cb2c37168730f3265ed64e301de44784ff7da55b01dd2cedef67af305

SHA-384:

3e8b29658d7646bd73dd8f234b7d0fe7a57c0e9b608d4d1c4b931bcb7265af9e6d0a520ff

Full Path:

C:\Users\forensic\Downloads\Win10_PC001.vmdk

Modified Time:

30/12/2023 15:34:01

Created Time:

30/12/2023 14:45:07

Entry Modified Time:

30/12/2023 17:31:50

File Size:

22.991.929.344

File Version:

Product Version:

Identical:

Extension:

vmdk

File Attributes:

A

OK

Para encontrar el hash de la evidencia hemos utilizado la herramienta HashMyfiles que nos ha permitido analizar la imagen y darnos todos los hashes que contiene el archivo.

3. Programa de control remoto

TeamViewer_Setup_x64.exe

Para conseguir el fichero .exe hemos estado revisando los ficheros de mft_parseo.csv que lo hemos podido leer utilizando las herramientas MFTECmd.exe y TimelineExplorer.exe.

Con MFTECmd.exe hemos generado el archivo .csv

```
C:\Herramientas\02_ZimmermanTools>MFTECmd.exe -f "C:\Users\forensic\Desktop\kape\E\MFT" --body "C:\Users\forensic\Desktop\kape\MFTE" --bodyf parseo_mft.body --blf --bdl c
MFTECmd version 1.2.2.1

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/MFTECmd

Command line: -f C:\Users\forensic\Desktop\kape\E\MFT --body C:\Users\forensic\Desktop\kape\MFTE --bodyf parseo_mft.body --blf --bdl c

Warning: Administrator privileges not found!

File type: Mft

Processed C:\Users\forensic\Desktop\kape\E\MFT in 10,9343 seconds

C:\Users\forensic\Desktop\kape\E\MFT: FILE records found: 157,054 (Free records: 95) File size: 153,5MB
Bodyfile output will be saved to C:\Users\forensic\Desktop\kape\MFTE\parseo_mft.body

C:\Herramientas\02_ZimmermanTools>
```

```
C:\Herramientas\02_ZimmermanTools>MFTECmd.exe -f "C:\Users\forensic\Desktop\kape\E\MFT" --csv "C:\Users\forensic\Desktop\kape\MFTE" --csvf mft_parseo.csv
MFTECmd version 1.2.2.1

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/MFTECmd

Command line: -f C:\Users\forensic\Desktop\kape\E\MFT --csv C:\Users\forensic\Desktop\kape\MFTE --csvf mft_parseo.csv

Warning: Administrator privileges not found!

File type: Mft

Processed C:\Users\forensic\Desktop\kape\E\MFT in 5,5810 seconds

C:\Users\forensic\Desktop\kape\E\MFT: FILE records found: 157,054 (Free records: 95) File size: 153,5MB
CSV output will be saved to C:\Users\forensic\Desktop\kape\MFTE\mft_parseo.csv

C:\Herramientas\02_ZimmermanTools>
```

En los pantallazos se muestran los comandos que hemos utilizado para genera el fichero .csv que es la ruta donde se encuentra la MFT que hemos podido extraer con kape.

Con TimelineExplorer.exe hemos podido leer los ficheros en una tabla.

Timeline Explorer v1.3.0.0				
File Tools Tabs View Help				
mft_parse.csv				
Arrastre una columna aquí para agrupar por dicha columna				
			Introduzca texto a buscar...	
			Buscar	
	In Use	Parent Path	File Name	
1	<input checked="" type="checkbox"/>	.\Users\Public	svchost.exe	
1	<input checked="" type="checkbox"/>	.\Users\Public	procdump64.exe	
1	<input checked="" type="checkbox"/>	.\Users\IEUser\Downloads	GoogleDriveSetup.exe	
1	<input checked="" type="checkbox"/>	.\Users\IEUser\Downloads	TeamViewer_Setup_x64.exe	
2	<input checked="" type="checkbox"/>	.\Users\IEUser\AppData\Local\Temp\TeamViewer	TeamViewer_.exe	
2	<input type="checkbox"/>	.\Users\IEUser\AppData\Local\Temp\dist\APTSimulator\helpers	curl.exe	
2	<input type="checkbox"/>	.\Users\IEUser\AppData\Local\Temp\dist\APTSimulator\helpers	7z.exe	
2	<input type="checkbox"/>	.\Users\IEUser\AppData\Local\Temp\APTSimulator\helpers	curl.exe	
2	<input type="checkbox"/>	.\Users\IEUser\AppData\Local\Temp\APTSimulator\helpers	7z.exe	
1	<input checked="" type="checkbox"/>	.\Users\IEUser\AppData\Local\Temp	sethc.exe	
2	<input checked="" type="checkbox"/>	.\Users\IEUser\AppData\Local\Microsoft\WindowsApps\Microsoft.XboxGamingOverlay_8wekyb3d8bbwe	GameBarElevatedFT_Alias.exe	
1	<input checked="" type="checkbox"/>	.\Users\IEUser\AppData\Local\Microsoft\WindowsApps\Microsoft.MicrosoftEdge_8wekyb3d8bbwe	MicrosoftEdge.exe	
2	<input checked="" type="checkbox"/>	.\Users\IEUser\AppData\Local\Microsoft\WindowsApps\Microsoft.DesktopAppInstaller_8wekyb3d8bbwe	winget.exe	
1	<input checked="" type="checkbox"/>	.\Users\IEUser\AppData\Local\Microsoft\WindowsApps	MicrosoftEdge.exe	
1	<input checked="" type="checkbox"/>	.\Users\IEUser\AppData\Local\Microsoft\WindowsApps	GameBarElevatedFT_Alias.exe	
1	<input checked="" type="checkbox"/>	.\Users\IEUser\AppData\Local\Microsoft\WindowsApps	winget.exe	
2	<input checked="" type="checkbox"/>	.\Users\IEUser\AppData\Local\Microsoft\OneDrive\Update	OneDriveSetup.exe	
4	<input checked="" type="checkbox"/>	.\Users\IEUser\AppData\Local\Microsoft\OneDrive\22.077.0410.0007	OneDriveSetup.exe	
4	<input checked="" type="checkbox"/>	.\Users\IEUser\AppData\Local\Microsoft\OneDrive\22.077.0410.0007	OneDriveUpdaterService.exe	
4	<input checked="" type="checkbox"/>	.\Users\IEUser\AppData\Local\Microsoft\OneDrive\22.077.0410.0007	OneDriveFileLauncher.exe	

Hemos deducido que el programa de control remoto era Teamviewer, ya que es una aplicación bastante conocida.

3.1 Fecha de descarga del fichero .exe

2022-04-29 17:11:25

Lo hemos localizado en la misma tabla donde hemos encontrado el fichero .exe

TeamViewer_Setup_x64.exe	.exe	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	37398984	2022-04-29 17:11:25
--------------------------	------	--------------------------	--------------------------	--------------------------	----------	---------------------

3.2 Fecha ejecución del fichero .exe

29/04/2022

Lo hemos localizado en la misma tabla donde hemos encontrado el fichero .exe

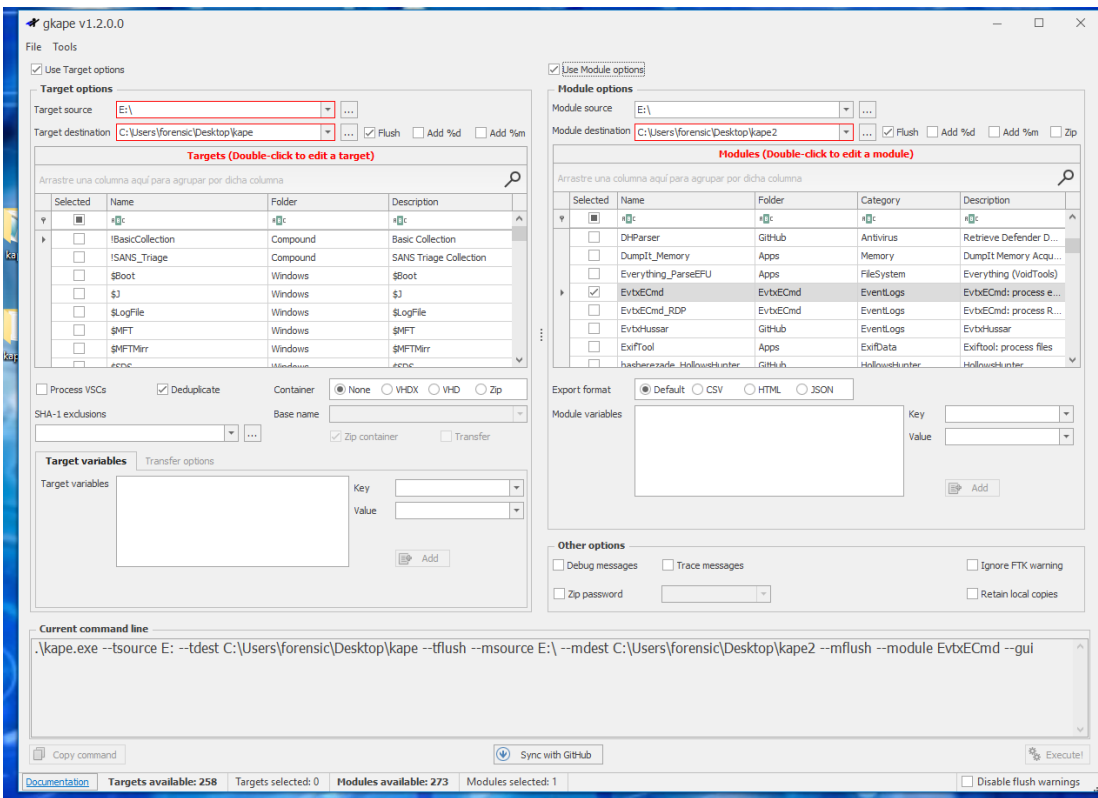
TeamViewer_Setup_x64.exe	.exe	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	37398984	2022-04-29 17:11:25
--------------------------	------	--------------------------	--------------------------	--------------------------	----------	---------------------

4. Fichero .ZIP eliminado

Cosas.zip

Para encontrar el fichero .Zip hemos utilizado varias herramientas.

La primera que hemos usado es KAPE.

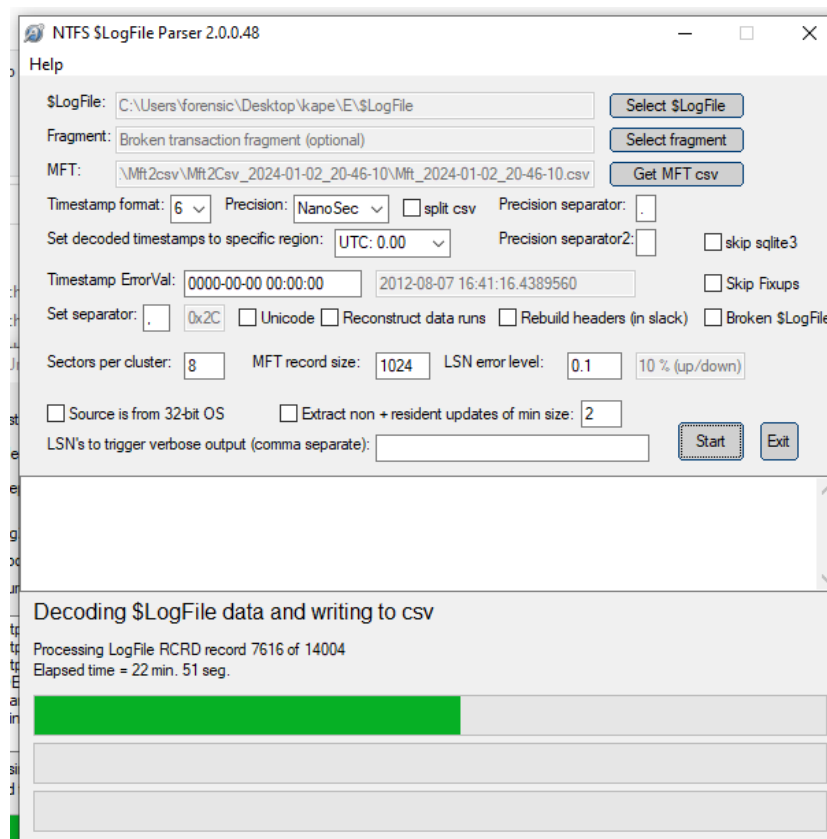
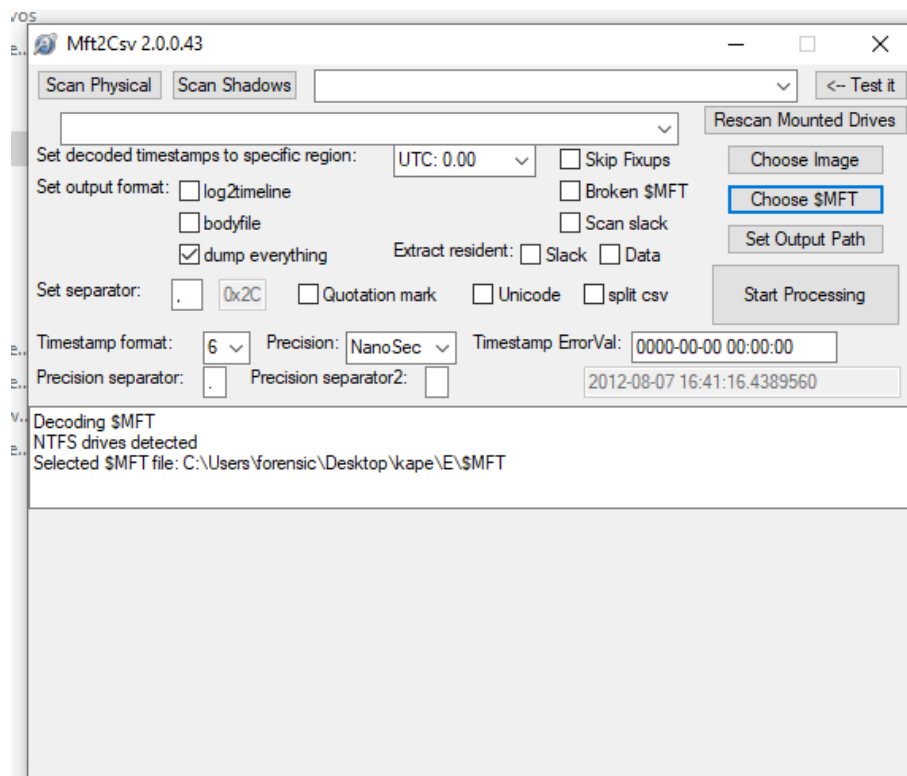


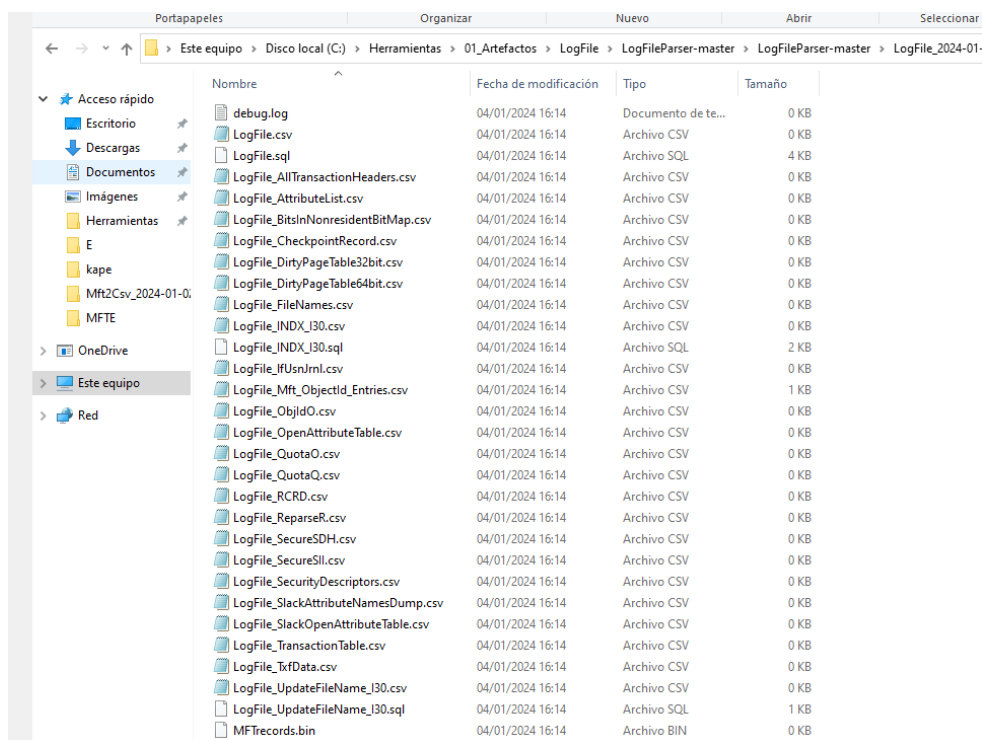
primero hemos ejecutado los targets y después las opciones de módulos, que hemos ejecutado la de EvtxECmd.

Al ejecutarlo nos ha extraído un fichero con varios logs igual que hicimos para encontrar el nombre de la máquina. Con kape se nos han creado varios archivos.

Nombre	Fecha de modificación	lipo	lamaño
\$Extend	30/12/2023 21:14	Carpeta de archivos	
\$Recycle.Bin	30/12/2023 21:12	Carpeta de archivos	
Program Files	30/12/2023 21:13	Carpeta de archivos	
ProgramData	30/12/2023 21:12	Carpeta de archivos	
Users	30/12/2023 21:12	Carpeta de archivos	
Windows	30/12/2023 21:13	Carpeta de archivos	
\$Boot	30/12/2023 21:14	Archivo	8 KB
\$LogFile	30/12/2023 21:14	Archivo	56.016 KB
\$MFT	19/03/2019 22:52	Archivo	157.184 KB
\$MFTMirr	30/12/2023 21:14	Archivo	4 KB
\$Secure_SSdS	19/03/2019 22:52	Archivo	2.316 KB

La siguiente herramienta que hemos utilizado para poder leer el fichero “\$Logfile” es la de “**NTFS \$Logfile Parser 2.0.0.48**”. Que lo que hemos hecho para que nos creara archivos .csv es seleccionar el fichero \$Logfile que había creado anterior mente con KAPE y seleccionar el fichero.csv de MFT que habíamos ejecutado con la herramienta de MFT MASTER (Mft2Csv 2.0.0.43).





Una vez ejecutado la herramienta “NTFS \$Logfile Parser 2.0.0.48”. Nos ha creado varios ficheros .csv para interpretarlo hemos utilizado la aplicación timeliner que hemos utilizado anteriormente, hemos seleccionado el archivo “**LogFile_Filenames.csv**” y hemos filtrado por .Zip y así es como hemos podido conseguir el fichero eliminado.

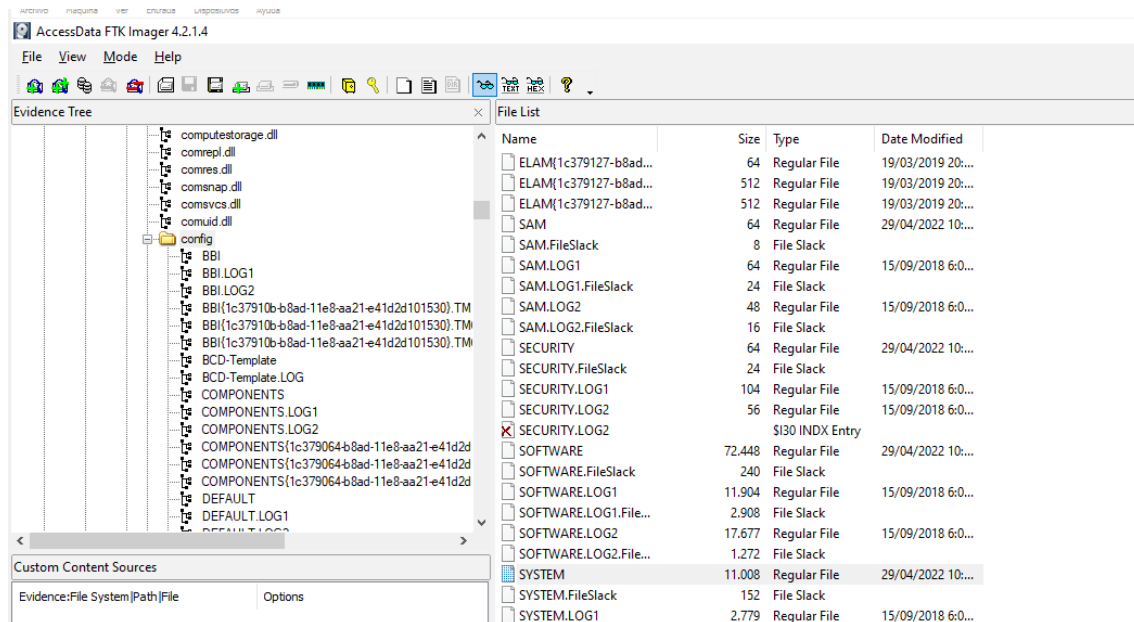
Timeline Explorer v1.3.0.0			
File Tools Tabs View Help			
LogFile_Filenames.csv			
Arrastre una columna aquí para agrupar por dicha columna			
	Line	Tag	Offset lf_LSN Mft Ref Mft Ref Seq No File Name
▼	=	■	=
▶	908	<input type="checkbox"/>	0x00CD20E8 622437405 156473 2 \$RQBJZQY.zip
	907	<input type="checkbox"/>	0x00CD1ED0 622437338 156473 2 cosas.zip
	906	<input type="checkbox"/>	0x00CD1D70 622437294 156473 2 \$RQBJZQY.zip
	905	<input type="checkbox"/>	0x00CD1CA0 622437268 156473 \$RQBJZQY.zip
	904	<input type="checkbox"/>	0x00CD0C20 622436740 82495 8 \$IQBJZQY.zip
	903	<input type="checkbox"/>	0x00CD0B58 622436715 82495 8 \$IQBJZQY.zip
	46	<input type="checkbox"/>	0x0024F6B0 621059798 156473 2 cosas.zip
	45	<input type="checkbox"/>	0x0024F5F0 621059774 156473 2 cosas.zip

5. Contraseñas débiles.

2d20d252a479f485cdf5e171d93985bf: qwerty

Para descubrir la contraseña de IEUser hemos utilizado las siguientes herramientas:

1º FTK Imager.



Hemos montado la imagen de la evidencia en la herramienta FTK para luego poder extraer los ficheros de **“SYSTEM”** y **“SAM”** que nos proporcionarán la información necesaria para poder sacar el hash de la contraseña. Estos ficheros se encuentran en la ruta root-windows-system32-config

2º MimiKatz

```
mimikatz 2.2.0 x64 (oe.eo)
Microsoft Windows [Versión 10.0.19044.3086]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Herramientas\mimikatz_trunk (2)\x64>mimikatz.exe

.#####. mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
.## ^ ##. "A la Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > https://blog.gentilkiwi.com/mimikatz
'## v #' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # lsadump::sam /system:C:\Users\forensic\Desktop\pruebas\SYSTEM /sam:C:\Users\forensic\Desktop\pruebas\SAM
Domain : PEGASUS01
SysKey : ec022a77f903a7e69e603e0c84634ff0
Local SID : S-1-5-21-321011808-3761883066-353627080

SAMKey : 939177c671faafb0f1d1f10bc6de1190

RID : 000001f4 (500)
User : Administrator
Hash NTLM: fc525c9683e8fe067095ba2ddc971889

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
Random Value : ee2d28072a728aa66eb25d67292cf6c5

* Primary:Kerberos-Newer-Keys *
Default Salt : MSEDGEWIN10Administrator
Default Iterations : 4096
```

```

cs mimikatz 2.2.0 x64 (oe.eo)
Default Iterations : 4096
Credentials
  aes256_hmac      (4096) : fb60f0d32a8abb7dd991ae530844c927fb25380ffffeb119ccd0971c5be8df321
  aes128_hmac      (4096) : e4617e2dd5e029348f552ece98695ddb
  des_cbc_md5      (4096) : 1ce9546ebf6e5e45

* Packages *
  NTLM-Strong-NTOWF

* Primary:Kerberos *
  Default Salt : WDAGUtilityAccount
  Credentials
    des_cbc_md5      : 1ce9546ebf6e5e45

RID : 000003e8 (1000)
User : IEUser
Hash NTLM: 2d20d252a479f485cdf5e171d93985bf

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
  Random Value : c6a807d33d3772144ce3407a8a73f9ef

* Primary:Kerberos-Newer-Keys *
  Default Salt : MSEDGEWIN10IEUser
  Default Iterations : 4096
  Credentials
    aes256_hmac      (4096) : 72cc752f2addce7556960ad819259738c4fd86e7130cee6b06aca1137ad1e6cb
    aes128_hmac      (4096) : 7d83280d0766f4ad6510460fbd975fbc
    des_cbc_md5      (4096) : ecd9340ddff7406b

```

La siguiente herramienta que hemos utilizado es mimikatz que utilizando los ficheros extraídos anteriormente de la evidencia (SYSTEM y SAM) ha podido extraer toda la información que contenía proporcionándonos los hashes con la contraseña de los usuarios. Para poder ejecutarlo hemos lanzado el siguiente comando con la ruta donde hemos guardado los ficheros extraídos.

"lsadump::sam/system:C:\Users\forensic\Desktop\pruebas\SYSTEM\sam:C:\Users\forensic\Desktop\pruebas\SAM"

3º CrackStation

Por último, hemos entrado en la siguiente web <https://crackstation.net/> que nos ha permitido descryptar el hash y poder leer la contraseña.

CrackStation
Password Hashing Security
Defuse Security

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

2d20d252a479f485cdf5e171d93985bf

☐ No soy un robot

Crack Hashes

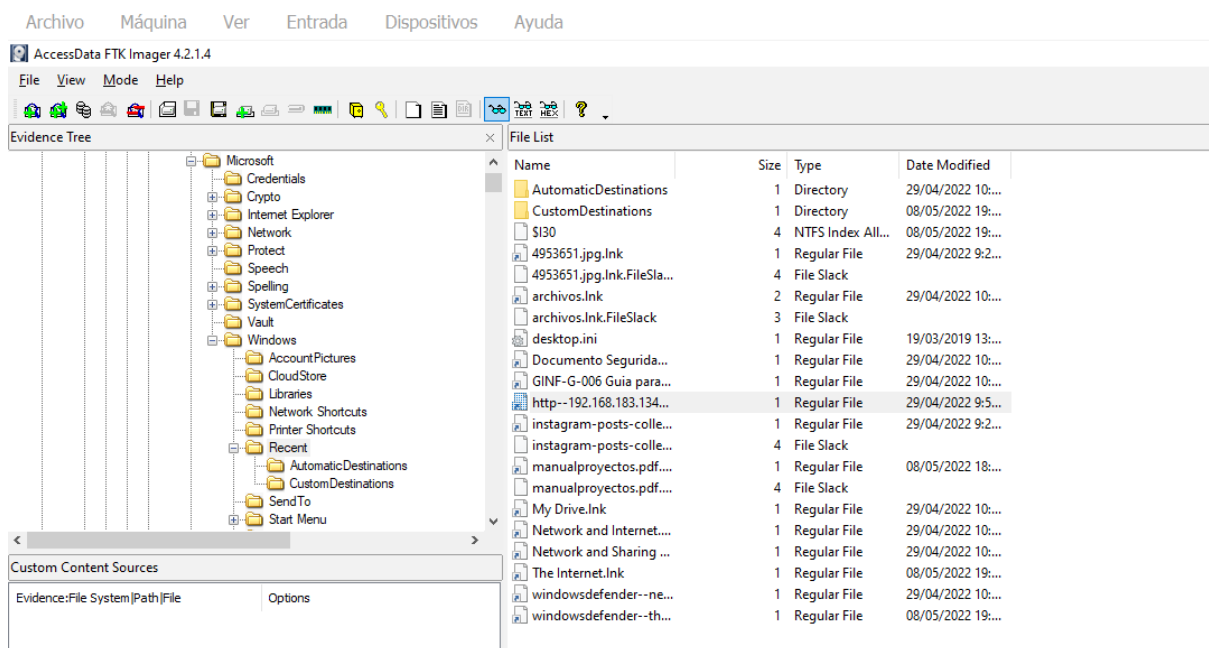
Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3.1BackupDefaults

Hash	Type	Result
2d20d252a479f485cdf5e171d93985bf	NTLM	qwerty

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

6. Conexión RDP

IP: 192.168.183.134



Para descubrir la ip donde se realizaba la conexión remota, lo que hemos hecho es investigar los diferentes ficheros que nos ha proporcionado la herramienta FTK cuando hemos extraído la evidencia. La ruta donde se encontraba la ip es la siguiente: root-Users-IEUser-AppData-Roaming-Microsoft-Windows-Recent y ahí nos hemos encontrado con un fichero que ponía la IP. Esta ruta la hemos deducido porque es donde se encuentran los registros de LNK que son ficheros que se crean cuando se abre algún archivo ya sea local o en remoto.

6.1 Puerto Conexión maquina

445

Para descubrir el puerto hemos utilizado una herramienta de Zimmerman que ya habíamos utilizado para encontrar el nombre de la máquina que es la de EvtxECmd.exe para ello hemos tenido que encontrar la ruta donde se encontraban los logs de RDP, que habíamos extraído anteriormente con la herramienta de kape como hemos visto en otros apartados.

C:\Users\forensic\Desktop\kape\E\Windows\System32\winevt\logs

```

C:\Windows\System32\cmd.exe
Microsoft Windows [Versión 10.0.19044.3086]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Herramientas\01_Artefactos\Eventos\EvtxECmd>EvtxECmd.exe -d C:\Users\forensic\Desktop\kape\E\Windows\System32\winevt\logs --csvf C:\Users\forensic\Desktop\extraido --csv evento_windows.csv
EvtxECmd version 1.0.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/evtX

Command line: -d C:\Users\forensic\Desktop\kape\E\Windows\System32\winevt\logs --csvf C:\Users\forensic\Desktop\extraido --csv evento_windows.csv

Warning: Administrator privileges not found!

Path to evento_windows.csv doesn't exist. Creating...
CSV output will be saved to evento_windows.csv\extraido

Maps loaded: 383
Looking for event log files in C:\Users\forensic\Desktop\kape\E\Windows\System32\winevt\logs

Processing C:\Users\forensic\Desktop\kape\E\Windows\System32\winevt\logs\Application.evtx...
Chunk count: 10, Iterating records...
Record #: 14 (timestamp: 2019-03-19 12:59:30.1351093): Warning! Time just went backwards! Last seen time before change: 2019-03-19 20:59:28.4554551
Record #: 752 (timestamp: 2022-04-29 08:27:06.3757601): Warning! Time just went backwards! Last seen time before change: 2022-04-29 17:18:00.6304835

Event log details
Flags: IsDirty
Chunk count: 10
Stored/Calculated CRC: 5B44D735/5B44D735
Earliest timestamp: 2019-03-19 12:59:29.4872244
Latest timestamp: 2022-05-08 19:11:16.2017415
Total event log records found: 978

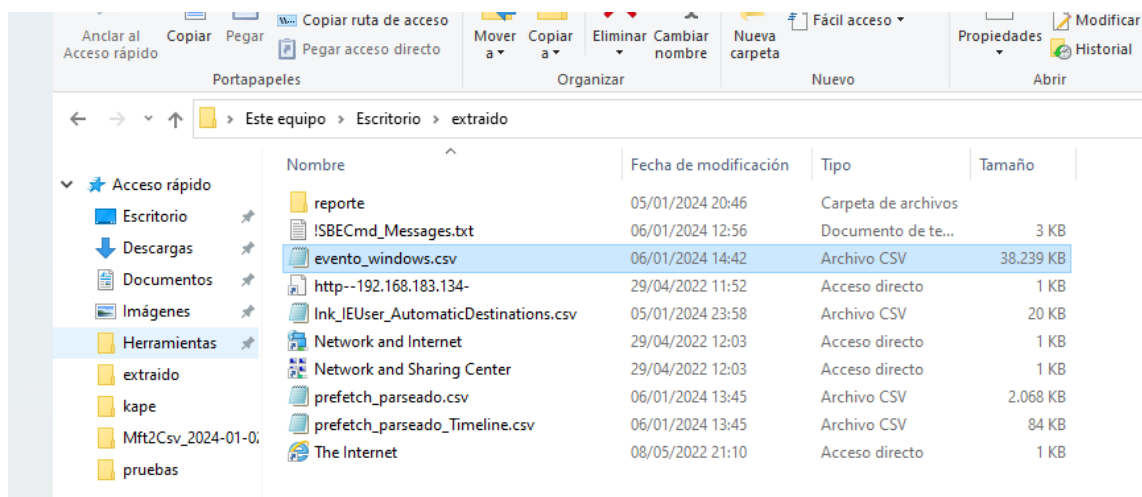
Records included: 978 Errors: 0 Events dropped: 0

```

Para ejecutar la herramienta hemos utilizado el siguiente comando

***“EvtxECmd>EvtxECmd.exe -d
C:\Users\forensic\Desktop\kape\E\Windows\System32\winevt\logs --
csvf C:\Users\forensic\Desktop\extraido --csv evento_windows.csv”***

Una vez ejecutado y analizado todos los archivos que se encontraban en la ruta nos ha generado un fichero.csv que hemos denominado evento_windows.csv



Para leer el fichero hemos utilizad timeliner y filtrando en remote Host hemos localizado la ip descubierta anterior mente con el puerto.

Timeline Explorer v1.3.0.0									
File Tools Tabs View Help									
hayabusas_export.csv									
Arrastre una columna aquí para agrupar por dicha columna									
Introduzca texto a buscar...									
Buscar									
Line	Tag	Timestamp	Computer	Channel	Event ID	Level	Record ID	Rule Title	Details
1		2019-03-19 14:21:34.056 +01:00	MSEDGEMIN10	PwSh	4103	high	68	Suspicious PowerShell Invocations - Specific - PowerShell Module	Payload: CommandInvocation(Add-Type): "Add-Ty
2		2019-03-19 21:57:23.437 +01:00	MSEDGEMIN10	Sec	4732	high	204	User Added To Local Admin Grp	SrcSID: S-1-5-21-321011808-3761883066-35362708
3		2019-03-19 21:59:25.364 +01:00	MSEDGEMIN10	Sec	4732	high	235	User Added To Local Admin Grp	SrcSID: S-1-5-21-321011808-3761883066-35362708
4		2022-05-08 21:04:52.827 +02:00	PEGASUS01	Defender	1116	high	105	Antivirus Relevant File Paths Alerts	Threat: Trojan:BAT/VigorF.A Severity: Severe
5		2022-05-08 21:04:52.827 +02:00	PEGASUS01	Defender	1116	crit	105	Defender Alert (Severe)	Threat: Trojan:BAT/VigorF.A Severity: Severe
6		2022-05-08 21:04:53.529 +02:00	PEGASUS01	Defender	1116	high	107	Antivirus Hacktool Detection	Threat: Trojan:Win32/PowerSploit!ml Severity: Severe
7		2022-05-08 21:04:53.529 +02:00	PEGASUS01	Defender	1116	high	107	Antivirus Relevant File Paths Alerts	Threat: Trojan:Win32/PowerSploit!ml Severity: Severe
8		2022-05-08 21:04:53.529 +02:00	PEGASUS01	Defender	1116	crit	107	Defender Alert (Severe)	Threat: Trojan:Win32/PowerSploit!ml Severity: Severe
9		2022-05-08 21:04:53.529 +02:00	PEGASUS01	Defender	1116	crit	107	Antivirus Exploitation Framework Detection	Threat: Trojan:Win32/PowerSploit!ml Severity: Severe
10		2022-05-08 21:04:56.552 +02:00	PEGASUS01	Defender	1116	high	108	Antivirus Relevant File Paths Alerts	Threat: Trojan:BAT/VigorF.A Severity: Severe
11		2022-05-08 21:04:56.552 +02:00	PEGASUS01	Defender	1116	crit	108	Defender Alert (Severe)	Threat: Trojan:BAT/VigorF.A Severity: Severe
12		2022-05-08 21:04:56.600 +02:00	PEGASUS01	Defender	1116	high	109	Antivirus Hacktool Detection	Threat: Trojan:Win32/PowerSploit!ml Severity: Severe
13		2022-05-08 21:04:56.600 +02:00	PEGASUS01	Defender	1116	high	109	Antivirus Relevant File Paths Alerts	Threat: Trojan:Win32/PowerSploit!ml Severity: Severe
14		2022-05-08 21:04:56.600 +02:00	PEGASUS01	Defender	1116	crit	109	Defender Alert (Severe)	Threat: Trojan:Win32/PowerSploit!ml Severity: Severe
15		2022-05-08 21:04:56.600 +02:00	PEGASUS01	Defender	1116	crit	109	Antivirus Exploitation Framework Detection	Threat: Trojan:Win32/PowerSploit!ml Severity: Severe
16		2022-05-08 21:06:33.528 +02:00	PEGASUS01	Defender	1116	high	113	Antivirus Relevant File Paths Alerts	Threat: Backdoor:PowerShell/Powercat.A Severity: Severe
17		2022-05-08 21:06:33.528 +02:00	PEGASUS01	Defender	1116	crit	113	Defender Alert (Severe)	Threat: Backdoor:PowerShell/Powercat.A Severity: Severe
18		2022-05-08 21:06:43.306 +02:00	PEGASUS01	Defender	1116	high	114	Defender Alert (High)	Threat: HackTool:Win32/Dumplings.E Severity: Severe
19		2022-05-08 21:06:43.306 +02:00	PEGASUS01	Defender	1116	high	114	Antivirus Hacktool Detection	Threat: HackTool:Win32/Dumplings.E Severity: Severe
20		2022-05-08 21:06:43.306 +02:00	PEGASUS01	Defender	1116	high	114	Antivirus Relevant File Paths Alerts	Threat: HackTool:Win32/Dumplings.E Severity: Severe
21		2022-05-08 21:06:43.306 +02:00	PEGASUS01	Defender	1116	crit	114	Antivirus Password Dumper Detection	Threat: HackTool:Win32/Dumplings.E Severity: Severe
22		2022-05-08 21:06:51.718 +02:00	PEGASUS01	Sec	4732	high	5710	User Added To Local Admin Grp	SrcSID: S-1-5-21-321011808-3761883066-35362708
23		2022-05-08 21:07:02.708 +02:00	PEGASUS01	Defender	1116	high	136	Antivirus Relevant File Paths Alerts	Threat: SettingsModifier:Win32/PossibleHostsF
24		2022-05-08 21:07:02.827 +02:00	PEGASUS01	Defender	1116	high	137	Antivirus Relevant File Paths Alerts	Threat: SettingsModifier:Win32/PossibleHostsF
25		2022-05-08 21:07:02.943 +02:00	PEGASUS01	Defender	1116	high	138	Antivirus Relevant File Paths Alerts	Threat: SettingsModifier:Win32/PossibleHostsF
26		2022-05-08 21:07:03.046 +02:00	PEGASUS01	Defender	1116	high	139	Antivirus Relevant File Paths Alerts	Threat: SettingsModifier:Win32/PossibleHostsF
27		2022-05-08 21:07:03.154 +02:00	PEGASUS01	Defender	1116	high	140	Antivirus Relevant File Paths Alerts	Threat: SettingsModifier:Win32/PossibleHostsF
28		2022-05-08 21:07:06.737 +02:00	PEGASUS01	Defender	1116	high	142	Antivirus Relevant File Paths Alerts	Threat: Trojan:Win32/Ceprolad.A Severity: Severe
29		2022-05-08 21:07:06.737 +02:00	PEGASUS01	Defender	1116	crit	142	Defender Alert (Severe)	Threat: Trojan:Win32/Ceprolad.A Severity: Severe

Con la herramienta timeline hemos abierto el fichero .csv que nos ha generado, hemos estado analizando el archivo y no hemos podido encontrar nada.

2º CHAINSAW

C:\Herramientas\chainsaw_all_platforms\rules\chainsawchainsaw_x86_64-pc-windows-msvc.exe hunt C:\Users\forensic\Desktop\kape\E\Windows\System32\winevt\logs -s sigma/ -r rules/ --mapping mappings/sigma-event-logs-all.yml

CHAINSAW
By WithSecure Countercept (@frantictyping, @alexkornitzer)

```
[+] Loading detection rules from: rules/, sigma/
[+] loaded 3100 detection rules (369 not loaded)
[+] Loading forensic artefacts from: C:\Users\forensic\Desktop\kape\E\Windows\System32\winevt\logs (extensions: .evtx, .evt)
[+] loaded 105 forensic artefacts (63.2 MB)
[+] Hunting: [=====] 105/105 -
[+] Group: Network Tampering
```

timestamp	detections	Event ID	Record ID	Computer	User	User SID	Member SID
2019-03-19 13:23:55	+ User Added to Global Group	4728	3586	MSEDGEMIN10	None		S-1-5-21-321011808-3761883066-353627080-1802
2019-03-19 13:23:55	+ New User Created	4720	3587	MSEDGEMIN10	sshd	S-1-5-21-321011808-3761883066-353627080-1802	
2019-03-19 20:55:22	+ User Added to Local Group	4732	32	IEUSER-F7QC4582	EIS_IUSRS		S-1-5-17
2019-03-19 20:55:22	+ User Added to Global Group	4728	41	IEUSER-F7QC4582	None		S-1-5-21-321011808-3761883066-353627080-1804
2019-03-19 20:55:22	+ New User Created	4720	42	IEUSER-F7QC4582	WDAGUtilityAccount	S-1-5-21-321011808-3761883066-353627080-1804	
2019-03-19 20:55:31	+ User Added to Local Group	4732	86	IEUSER-F7QC4582	Users		S-1-5-4
2019-03-19 20:55:31	+ User Added to Local Group	4732	87	IEUSER-F7QC4582	Users		S-1-5-11
2019-03-19 20:57:23	+ User Added to Global Group	4728	194	MSEDGEMIN10	None		S-1-5-21-321011808-3761883066-353627080-1800
2019-03-19 20:57:23	+ New User Created	4720	195	MSEDGEMIN10	IEUser	S-1-5-21-321011808-3761883066-353627080-1800	
2019-03-19 20:57:23	+ User Added to Local Group	4732	198	MSEDGEMIN10	Users		S-1-5-21-321011808-3761883066-353627080-1800
2019-03-19 20:57:23	+ User Added to Local Group	4732	204	MSEDGEMIN10	Administrators		S-1-5-21-321011808-3761883066-353627080-1800
2019-03-19 20:59:25	+ User Added to Global Group	4728	224	MSEDGEMIN10	None		S-1-5-21-321011808-3761883066-353627080-1801
2019-03-19 20:59:25	+ New User Created	4720	225	MSEDGEMIN10	defaultuser0	S-1-5-21-321011808-3761883066-353627080-1801	

La segunda herramienta que hemos utilizado para ver si podíamos encontrar el ID de la maquina desde donde se conectaba el atacante es de la Chainsaw que igual que la de hayabusas hemos usado la ruta donde se encuentran los logs de RDP.

C:\Users\forensic\Desktop\kape\E\Windows\System32\winevt\logs

Para ejecutar el programa utilizamos el siguiente comando:

"chainsaw_x86_64-pc-windows-msvc.exe hunt

C:\Users\forensic\Desktop\kape\E\Windows\System32\winevt\logs -s sigma/ -r rules/ --mapping mappings/sigma-event-logs-all.yml"

Una vez ejecutado nos ha generado una tabla con las distintas reglas que utiliza el programa como por ejemplo sigma, hemos estado analizando la tabla e intentado descubrir el id y no lo hemos conseguido.

[+] Group: Login Attacks					
timestamp	detections	count	Event ID	User	
2022-04-29 08:34:59	+ Account Brute Force	6	4625	IEUser	

[+] Group: Microsoft RDS Events - User Profile Disk					
timestamp	detections	Event ID	Channel	Computer	Information
2019-03-19 12:59:30	+ User Profile Disk - Registry file loaded	5	Microsoft-Windows-User Profile Service/Operational	MSEDGWIN10	C:\Users\defaultuser0\AppData\Local\Microsoft\Windows\UsrClass.dat
2019-03-19 12:59:36	+ User Profile Disk - Registry file loaded	5	Microsoft-Windows-User Profile Service/Operational	MSEDGWIN10	C:\Users\defaultuser0\ntuser.dat
2019-03-19 12:59:36	+ User Profile Disk - Registry file loaded	5	Microsoft-Windows-User Profile Service/Operational	MSEDGWIN10	C:\Users\defaultuser0\AppData\Local\Microsoft\Windows\UsrClass.dat
2019-03-19 13:00:05	+ User Profile Disk - Registry file loaded	5	Microsoft-Windows-User Profile Service/Operational	MSEDGWIN10	C:\Users\IEUser\ntuser.dat
2019-03-19 13:00:05	+ User Profile Disk - Registry file loaded	5	Microsoft-Windows-User Profile Service/Operational	MSEDGWIN10	C:\Users\IEUser\AppData\Local\Microsoft\Windows\UsrClass.dat
2019-03-19 13:01:16	+ User Profile Disk - Registry file loaded	5	Microsoft-Windows-User Profile Service/Operational	MSEDGWIN10	C:\Users\IEUser\ntuser.dat
2019-03-19 13:01:16	+ User Profile Disk - Registry file loaded	5	Microsoft-Windows-User Profile Service/Operational	MSEDGWIN10	C:\Users\IEUser\AppData\Local\Microsoft\Windows\UsrClass.dat
2019-03-19 13:07:02	+ User Profile Disk - Registry file loaded	5	Microsoft-Windows-User Profile Service/Operational	MSEDGWIN10	C:\Users\IEUser\ntuser.dat
2019-03-19 13:07:02	+ User Profile Disk - Registry file loaded	5	Microsoft-Windows-User Profile Service/Operational	MSEDGWIN10	C:\Users\IEUser\AppData\Local\Microsoft\Windows\UsrClass.dat

Aquí un ejemplo de los datos que nos ha sacado Chainsaw y hemos tratado de analizar.

8.Fichero maliciosos

La carpeta donde se encontraban los ficheros maliciosos tampoco hemos conseguido donde encontrarla. Lo hemos intentado usando las siguientes herramientas.

1º EvtxECmd.exe


```
C:\Windows\System32\cmd.exe
```

```
Microsoft Windows [Versión 10.0.19044.3886]
```

```
(c) Microsoft Corporation. Todos los derechos reservados.
```

```
C:\Herramientas\01_Artefactos\Eventos\EvtxECmd>EvtxECmd.exe -d C:\Users\forensic\Desktop\kape\E\Windows\System32\winevt\logs --csvf C:\Users\forensic\Desktop\extraido --csv evento_windows.csv
EvtxECmd version 1.0.0.0
```

```
Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/evtX
```

```
Command line: -d C:\Users\forensic\Desktop\kape\E\Windows\System32\winevt\logs --csvf C:\Users\forensic\Desktop\extraido --csv evento_windows.csv
```

```
Warning: Administrator privileges not found!
```

```
Path to evento_windows.csv doesn't exist. Creating...
CSV output will be saved to evento_windows.csv\extraido
```

```
Maps loaded: 383
```

```
Looking for event log files in C:\Users\forensic\Desktop\kape\E\Windows\System32\winevt\logs
```

```
Processing C:\Users\forensic\Desktop\kape\E\Windows\System32\winevt\logs\Application.evtx...
```

```
Chunk count: 10, Iterating records...
```

```
Record #: 14 (timestamp: 2019-03-19 12:59:30.1351093): Warning! Time just went backwards! Last seen time before change: 2019-03-19 20:59:28.4554551
```

```
Record #: 752 (timestamp: 2022-04-29 08:27:06.3757601): Warning! Time just went backwards! Last seen time before change: 2022-04-29 17:18:00.6304835
```

```
Event log details
```

```
Flags: IsDirty
```

```
Chunk count: 10
```

```
Stored/Calculated CRC: 5B44D735/5B44D735
```

```
Earliest timestamp: 2019-03-19 12:59:29.4872244
```

```
Latest timestamp: 2022-05-08 19:11:16.2017415
```

```
Total event log records found: 978
```

```
Records included: 978 Errors: 0 Events dropped: 0
```

Hemos utilizado la ruta donde se encontraban los logs de RDP:

C:\Users\forensic\Desktop\kape\E\Windows\System32\winevt\logs

Y luego lo hemos ejecutado con el siguiente comando:

"EvtxECmd>EvtxECmd.exe -d

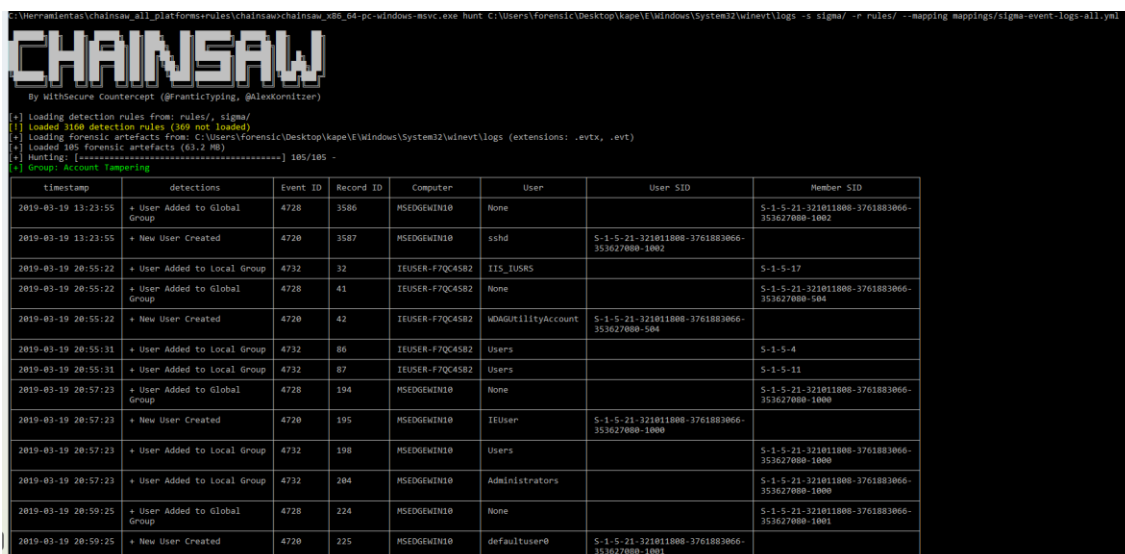
C:\Users\forensic\Desktop\kape\E\Windows\System32\winevt\logs --
csvf C:\Users\forensic\Desktop\extraido --csv evento_windows.csv"

Con este comando hemos generado un fichero .csv que hemos abierto con Timeliner.

Arrastre una columna aquí para agrupar por dicha columna										
Line	Tag	Record Number	Event Record Id	Time Created	Event Id	Level	Provider	Channel	Process Id	Computer
11279		6		6 2022-04-29 08:...	100	Critical	Microsoft-Windows-Diagnosis-Scheduled	Microsoft-Windows-Diagno...	7284	PEGASUS01
11298		13		13 2019-03-19 13:...	100	Critical	Microsoft-Windows-Diagnostics-Performa...	Microsoft-Windows-Diagno...	2584	MSEDGEWIN10
11299		14		14 2019-03-19 13:...	101	Critical	Microsoft-Windows-Diagnostics-Performa...	Microsoft-Windows-Diagno...	2584	MSEDGEWIN10
11389		24		24 2022-04-29 18:...	200	Critical	Microsoft-Windows-Diagnostics-Performa...	Microsoft-Windows-Diagno...	2396	PEGASUS01
12295		1		1 2019-03-19 20:...	1001	Critical	Microsoft-Windows-International	Microsoft-Windows-Intern...	2340	IEUSER-F7QC45B2
12296		2		2 2019-03-19 20:...	1001	Critical	Microsoft-Windows-International	Microsoft-Windows-Intern...	3344	IEUSER-F7QC45B2
12297		3		3 2019-03-19 20:...	1001	Critical	Microsoft-Windows-International	Microsoft-Windows-Intern...	3344	IEUSER-F7QC45B2
12298		4		4 2019-03-19 20:...	1001	Critical	Microsoft-Windows-International	Microsoft-Windows-Intern...	3344	IEUSER-F7QC45B2
12299		5		5 2019-03-19 20:...	1001	Critical	Microsoft-Windows-International	Microsoft-Windows-Intern...	3344	IEUSER-F7QC45B2
12300		6		6 2019-03-19 20:...	1001	Critical	Microsoft-Windows-International	Microsoft-Windows-Intern...	3344	IEUSER-F7QC45B2
12301		7		7 2019-03-19 20:...	1001	Critical	Microsoft-Windows-International	Microsoft-Windows-Intern...	3344	IEUSER-F7QC45B2
12302		8		8 2019-03-19 20:...	1001	Critical	Microsoft-Windows-International	Microsoft-Windows-Intern...	3344	IEUSER-F7QC45B2
12303		9		9 2019-03-19 20:...	1001	Critical	Microsoft-Windows-International	Microsoft-Windows-Intern...	3344	IEUSER-F7QC45B2
12304		10		10 2019-03-19 20:...	1001	Critical	Microsoft-Windows-International	Microsoft-Windows-Intern...	3344	IEUSER-F7QC45B2
12305		11		11 2019-03-19 20:...	1001	Critical	Microsoft-Windows-International	Microsoft-Windows-Intern...	3344	IEUSER-F7QC45B2
12306		12		12 2019-03-19 20:...	1001	Critical	Microsoft-Windows-International	Microsoft-Windows-Intern...	3344	IEUSER-F7QC45B2
12307		13		13 2019-03-19 20:...	1001	Critical	Microsoft-Windows-International	Microsoft-Windows-Intern...	3344	IEUSER-F7QC45B2
12308		14		14 2019-03-19 20:...	1001	Critical	Microsoft-Windows-International	Microsoft-Windows-Intern...	3344	IEUSER-F7QC45B2
12309		15		15 2019-03-19 20:...	1001	Critical	Microsoft-Windows-International	Microsoft-Windows-Intern...	3344	IEUSER-F7QC45B2
12310		16		16 2019-03-19 20:...	1001	Critical	Microsoft-Windows-International	Microsoft-Windows-Intern...	3344	IEUSER-F7QC45B2
12311		17		17 2019-03-19 20:...	1001	Critical	Microsoft-Windows-International	Microsoft-Windows-Intern...	3344	IEUSER-F7QC45B2
12312		18		18 2019-03-19 20:...	1001	Critical	Microsoft-Windows-International	Microsoft-Windows-Intern...	3344	IEUSER-F7QC45B2
12313		19		19 2019-03-19 20:...	1001	Critical	Microsoft-Windows-International	Microsoft-Windows-Intern...	3344	IEUSER-F7QC45B2
12314		20		20 2019-03-19 20:...	1001	Critical	Microsoft-Windows-International	Microsoft-Windows-Intern...	3344	IEUSER-F7QC45B2
12315		21		21 2019-03-19 20:...	1001	Critical	Microsoft-Windows-International	Microsoft-Windows-Intern...	3344	IEUSER-F7QC45B2
12316		22		22 2019-03-19 20:...	1001	Critical	Microsoft-Windows-International	Microsoft-Windows-Intern...	3344	IEUSER-F7QC45B2
12317		23		23 2019-03-19 20:...	1001	Critical	Microsoft-Windows-International	Microsoft-Windows-Intern...	3344	IEUSER-F7QC45B2
12318		24		24 2019-03-19 20:...	1001	Critical	Microsoft-Windows-International	Microsoft-Windows-Intern...	3344	IEUSER-F7QC45B2
12319		25		25 2019-03-19 20:...	1001	Critical	Microsoft-Windows-International	Microsoft-Windows-Intern...	3344	IEUSER-F7QC45B2

2º CHAINSAW

```
C:\Herramientas\chainsaw_all_platforms\rules\chainsaw\chainsaw_x86_64-pc-windows-msvc.exe hunt C:\Users\forensic\Desktop\kape\E\Windows\System32\winevt\logs -s sigma/ -r rules/ --mapping mappings/sigma-event-logs-all.yml
```



CHAINSAW
By WithSecure Countercept (@franticTyping, @alexkornitzer)

```
[*] Loading detection rules from: rules/, sigma/
[*] Loaded 3160 detection rules (369 not loaded)
[*] Loading forensic artefacts from: C:\Users\forensic\Desktop\kape\E\Windows\System32\winevt\logs (extensions: .evtx, .evt)
[*] Loaded 140 forensic artefacts (63/2 MB)
[*] Hunting: [-----] 105/105 -
[*] Group: Account Tampering
```

timestamp	detections	Event ID	Record ID	Computer	User	User SID	Member SID
2019-03-19 13:23:55	+ User Added to Global Group	4728	3586	MSEDGEWIN10	None		S-1-5-21-321011808-3761883066-353627000-1002
2019-03-19 13:23:55	+ New User Created	4720	3587	MSEDGEWIN10	sshd	S-1-5-21-321011808-3761883066-353627000-1002	
2019-03-19 20:55:22	+ User Added to Local Group	4732	32	IEUSER-F7QC45B2	IIS_IUSRS		S-1-5-17
2019-03-19 20:55:22	+ User Added to Global Group	4728	41	IEUSER-F7QC45B2	None		S-1-5-21-321011808-3761883066-353627000-504
2019-03-19 20:55:22	+ New User Created	4720	42	IEUSER-F7QC45B2	WDAGUtilityAccount	S-1-5-21-321011808-3761883066-353627000-504	
2019-03-19 20:55:31	+ User Added to Local Group	4732	86	IEUSER-F7QC45B2	Users		S-1-5-4
2019-03-19 20:55:31	+ User Added to Local Group	4732	87	IEUSER-F7QC45B2	Users		S-1-5-11
2019-03-19 20:57:23	+ User Added to Global Group	4728	194	MSEDGEWIN10	None		S-1-5-21-321011808-3761883066-353627000-1000
2019-03-19 20:57:23	+ New User Created	4720	195	MSEDGEWIN10	IEUser	S-1-5-21-321011808-3761883066-353627000-1000	
2019-03-19 20:57:23	+ User Added to Local Group	4732	198	MSEDGEWIN10	Users		S-1-5-21-321011808-3761883066-353627000-1000
2019-03-19 20:57:23	+ User Added to Local Group	4732	204	MSEDGEWIN10	Administrators		S-1-5-21-321011808-3761883066-353627000-1000
2019-03-19 20:59:25	+ User Added to Global Group	4728	224	MSEDGEWIN10	None		S-1-5-21-321011808-3761883066-353627000-1001
2019-03-19 20:59:25	+ New User Created	4720	225	MSEDGEWIN10	defaultuser0	S-1-5-21-321011808-3761883066-353627000-1001	

Hemos vuelto a utilizar la herramienta Chainsaw pero esta vez hemos generado ficheros .csv el comando utilizado es:

"chainsaw_x86_64-pc-windows-msvc.exe hunt C:\Users\forensic\Desktop\kape\E\Windows\System32\winevt\logs -s sigma/ -r rules/ --mapping mappings/sigma-event-logs-all.yml -o C:\Users\forensic\Desktop\extraido\chainsaw_export.csv --csv"

Portapapeles

Organizar

Nuevo

Abrir

←

→

⌵

⬆

📁

> Este equipo > Escritorio > extraido > chainsaw_export.csv

⌵

📌 Acceso rápido

📁 Escritorio

📁 Descargas

📁 Documentos

📁 Imágenes

📁 Herramientas

📁 chainsaw_export.cs

📁 extraido

📁 Mft2Csv_2024-01-0

Nombre

Fecha de modificación

Tipo

Tamaño

📄 account_tampering.csv

06/01/2024 19:24

Archivo CSV

4 KB

📄 antivirus.csv

06/01/2024 19:24

Archivo CSV

38 KB

📄 login_attacks.csv

06/01/2024 19:24

Archivo CSV

1 KB

📄 microsoft_rds_events_-_user_profile_disk....

06/01/2024 19:24

Archivo CSV

10 KB

📄 powershell_script.csv

06/01/2024 19:24

Archivo CSV

15 KB

📄 rdp_events.csv

06/01/2024 19:24

Archivo CSV

5 KB

📄 sigma.csv

06/01/2024 19:24

Archivo CSV

672 KB

Nos generó los siguientes ficheros .csv que estuvimos analizando uno por uno pero sin lograr conseguir la carpeta.